Testimony to AHIC CPS Work Group

Submitted by:

Cassi Birnbaum, RHIA, CPHQ
Director of Health Information and Privacy Officer
Rady Children's Hospital and Health Center
3020 Children's Way, Mailcode 5049
San Diego, CA 92123
Phone: 858-966-4095
Fax: 858-966-6737
eMail: ***cbirnbaum@rchsd.org***

As an active participant in the CalRHIO Privacy/Security Solutions Group after I was selected from the Regional Focus Groups over a year ago, it was my opinion as well as others who participated at the state level, that one of the significant barriers to full RHIO/HIE implementation is the implication of covered vs. non-covered entities participating in health information exchange. Additionally, in California, we have the additional complexity of state laws that layer onto the HIPAA regulations. In order to mitigate this concern there was consensus around the establishment of an oversight committee, Privacy and Security Advisory Board (PSAB) to establish the necessary infrastructure to set privacy policies and security standards for HIE. The solutions we came up with to address this concern included the development and use of standard business practice documents and health information content including:

- Business Associate Agreements (BAAs) with standard privacy and security language
- Health record content
- Standard contract language between vendors and providers
- Notice of Privacy Practices (NPPs) in a standard, easy to read format, and
- Authorization and consent documents in a standard, easy to read, and HIPAA and State Law compliant format.

During my involvement with CalRHIO and our final report identified three business practice variations: [1]

Covered vs. non-covered entities: HIPAA creates a distinction within the healthcare industry among entities handling individually identifiable health information resulting in or creating the potential for practice and disclosure variations, among covered and non-covered entities. There was consensus among the stakeholders that there is wide variation in practice with disclosing health information and differences with security protections between covered and non-covered entities. There was definitely cause for alarm from our consumer advocates who participated in these important discussions.

---

[1] "Privacy and Security Solutions of Interoperable Health Information Exchange", California's Final Assessment of Variations and Analysis of Solutions, prepared by: CalOHI & CalRHIO California Team, April 16, 2007, page 13.

There was definitely consensus among the stakeholders that privacy and security protections should be applied to health care information, not the entities handling the data. If this were the case, providers, other covered entities and consumer concerns would be addressed and the risks of improper disclosure would be greatly mitigated. As it relates to national health information exchange and the hosting of personal health records, the HIPAA privacy and security regulations should be the floor, with additional protections layered on if deemed necessary.

However, there are issues that would need to be addressed upfront related to other federal laws, i.e. FERPA and ERISA. Also, minors privacy rights which HIPAA defers to the states to govern access, produces a myriad of challenges related to participation in a RHIO/HIE effort. If an NPP is signed by the parent or if an "opt out" approach is used and the parent opts in, what happens when the child turns 18? Does right of access roll over? State laws vary regarding emancipated minors, guardian rights, confidential treatment, etc.

Also there was variation in operational practice among covered entities stemming from various interpretations and understanding of HIPAA, state law and their intersection. As a result, stakeholders reported business practice variations that result from different approaches to implement optimal and addressable provisions in HIPAA. [2]

Legal Complexity:

During our initial Regional Meeting as well as our numerous deliberations regarding privacy/security solutions for CalRHIO we discussed the myriad of State laws governing the privacy of medical information, which are further complicated by HIPAA preemption. This results in a variety of legal interpretations and widespread variation among business practices and policies directing the use and disclosure of medical information.[3] This was most prevalent in rural areas or communities which did not have the opportunity to participate in collaborative sharing regarding health information exchange. Also, small provider practices are often times disconnected from provider networks and do not have the tools or resources to assure well developed processes to facilitate compliance. National Providers and Payers in California have unique challenges with information exchanged across state lines, which could be mitigated if a uniform privacy/security standard was approved for use with RHIOs and HIE efforts.

Data Architecture:

There are no data architecture or data classification systems that can adequately identify and separate health information to assure that only the minimum necessary information

---

[2] "Privacy and Security Solutions of Interoperable Health Information Exchange", California's Final Assessment of Variations and Analysis of Solutions, prepared by: CalOHI & CalRHIO California Team, April 16, 2007, page 13.

[3] "Privacy and Security Solutions of Interoperable Health Information Exchange", California's Final Assessment of Variations and Analysis of Solutions, prepared by: CalOHI & CalRHIO California Team, April 16, 2007, page 13

for the purpose of the request was shared. [4] Furthermore, if a disclosure restriction was approved or in the case of a minor's record who was legally able to consent for treatment for a condition, i.e. pregnancy how can this be flagged in the record? If HIPAA is used as the floor for a provider, how would drug and alcohol treatment be ferreted out? As a Stakeholder from a Pediatric integrated delivery system how would minor records be disclosed to parents and how would custody be verified?

Trust as a Barrier to HIE

The overarching theme and barrier to Health Information Exchange is trust among stakeholders. One factor that may inhibit the development of HIE privacy and security standards is the 'tension" that results from conflicting goals between the patient's right to privacy and the provider's responsibility to disclose health care for payment and healthcare operations. The major factors related to trust include:

- Trust among providers to assure the same level of privacy and security of health information is maintained at all participating facilities
- Trust among providers and patients to assure the quality, accuracy, timeliness, availability and consistency of patient information
- Trust that HIE system access is limited to only those with a legitimate purpose
- Patients trust that their information will not be breached or used inappropriately

Other Issues Related to HIE

If I were involved in a non-covered entity's exchange of information or a PHR initiative, sound business practices would include protecting consumer privacy. Although, not specifically required, it would not be in any company's best interest to have sloppy practices associated with the most sensitive of information. As a consumer I would not participate in e-commerce if a .com has a questionable business history from a security/privacy standpoint. There is such palpable concern among Californians with identity and medical identify theft, that private PHR companies are at a major disadvantage, with the payer community running a close second. It is my prediction that companies who will survive and thrive in the era of heath information exchange can overcome the barrier of consumer concern through proven and transparent sound practices in the areas of security and privacy protections.

In order to facilitate design, implementation and oversight it is critical that all participating organizations be held to same standard of HIPAA privacy and security regulations, bound by a standard contract, either in a memorandum of understanding or a Business Associate Agreement format and overseen by a Privacy and Security Board.

[4] "Privacy and Security Solutions of Interoperable Health Information Exchange", California's Final Assessment of Variations and Analysis of Solutions, prepared by: CalOHI & CalRHIO California Team, April 16, 2007, page 13.

During my CalRHIO participation one area of consensus quickly reached by all stakeholders revolved around exchange of information in emergency medical situations where time is of the essence. In this scenario, the minimum necessary rule of HIPAA does not apply. If a Notice of Privacy Practice (NPP) or an opt out process is utilized to assure consumer notification, there should be language around an emergency treatment exception. Other types of exchange for routine care, treatment, pharmacy refills, diagnostic and therapeutic testing and interventions, payer inquiries, public health inquiries and disclosures, would require a NPP or a clear-cut opt out process. Disclosure for non-mandated public health inquiries, research and secondary uses of data would require an authorization. We had stakeholders from the mental and behavioral health sector who were concerned about the exposure if this information was shared. Applying HIPAA privacy protections and assuring that access and security controls were appropriately layered addressed many of these stakeholders concerns.

An HIE initiative needs to strive for consistency in the uses and disclosures of data and in the standards related to the data. Data submitted by entities that have privacy policies more stringent than legally required can cause inconsistent practice in how health information is treated (e.g., some entities may not allow their data to be used for research purposes or healthcare operations of other entities). This issue adds costs and are burdensome and risky for the HIE to administer.